CLAIMS:

1. A method of enabling selection of one or more pieces of secret information stored in a first entity, the first entity also storing at least one value indicative of at least one attribute for each of the one or more pieces of secret information, the method comprising the steps of:

(a) receiving at the first entity a request from a second entity for one or more of the values for one or more of the pieces of secret information stored in the first entity; and

(b) in response to the request, outputting the values to the second entity.

2. A method according to claim 1 wherein each of the pieces of secret information has an associated index and the request in step (a) includes one or more of the indexes to identify those pieces of secret information for which the values are requested.

3. A method according to claim 1 wherein the request in step (a) is a request for the values all of the pieces of secret information and the response in step (b) orders the values such that the second entity can determine which values are associated with which piece of secret information, and can use the order to generate an index for the secret information.

4. A method according to claim 2 or claim 3, further including the steps, in the first entity and following step (b), of:

(c) receiving a request from the second entity identifying a function and identifying the index of a piece of secret information to be used in performing the function; and

(d) performing the function using the identified piece of secret information.

5. A method according to claim 1, further including the steps, in the first entity and following step (b), of:

(c) receiving a request from the second entity identifying a function and a piece of secret information to be used in performing the function; and

(d) performing the function using at least the identified piece of secret information, the identified piece of secret information being identified in the request of step (c) on the basis of at least one of the values output in step (b).

6. A method according to claim 1, wherein the secret information is stored in one or more physical locations of the first entity, and wherein the values are not indicative of those physical locations.

7. A method according to claim 1, wherein the first entity is implemented in a first integrated circuit and the second entity is implemented in a second integrated circuit.

8. A method according to claim 7, wherein the first integrated circuit includes a memory for storing the pieces of secret information and the values.

9. A method according to claim 8, including a plurality of the first integrated circuits, wherein the physical location of a piece of the secret information having particular attributes is mutually different for at least some of the first integrated circuits.

10. A method according to claim 1, wherein each of the pieces of secret information is a key for use with a corresponding authentication, encryption or decryption function.

11. A method according to claim 10, wherein the integrated circuit is programmed and configured to apply at least one of the authentication, encryption or decryption functions to data using the corresponding key as an operand.

12. A method according to claim 1, wherein the attribute stored for at least one of the pieces of secret information is the length of that at least one of the pieces of secret information.

13. A method according to claim 10, wherein the attribute stored for at least one of the pieces of secret information is the authentication, encryption or decryption type associated with that at least one of the pieces of secret information.

14. A method according to claim 1, wherein the attribute value stored for at least one of the pieces of secret information is indicative of a permission associated with that at least one of the pieces of secret information.

15. A system including first and second integrated circuits, the first integrated circuit implementing the first entity of claim 1, the second integrated circuit being programmed and configured to issue a request to the first integrated circuit for attribute values of any secret information stored by the first integrated circuit, and the first integrated circuit being programmed and configured to respond to the request by supplying the attribute values of the pieces of secret information to the external source.

16. A system according to claim 15, wherein the second integrated circuit is a printer controller chip and the first integrated circuit is a peripheral chip in communication with the printer controller.

17. A system according to claim 16, wherein the printer controller chip is installed in a printer and the peripheral chip is in a package that is releasably attachable to the printer via a connector, the connector enabling communication between the printer controller chip and the peripheral chip.

18. A system according to claim 16, wherein the printer controller chip and the peripheral chip are installed in a printer.

19. A system according to claim 17, wherein the package is an ink refill cartridge.

20. A system according to claim 17, wherein the package is a performance setting cartridge configured to set a performance level of the printer.

21. A system according to claim 15, wherein in the event at least one of the pieces of secret information can be altered or updated, the first integrated circuit is configured to alter the attribute values associated with that at least one piece of secret information as required by the alteration or update such that the update or alteration of the at least one piece of secret information and its associated attributes is atomic.